AU/ACSC/2016

AIR COMMAND STAFF COLLEGE

AIR UNIVERSITY

ART OF THE POSSIBLE: SECURING AIR FORCE SPACE COMMAND MISSION SYSTEMS FOR THE WARFIGHTER

By

Timothy P. Noonan, GS-13, DAFC

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Marcia Ledlow

Maxwell Air Force Base, Alabama

23 October 2016

DISTRIBUTION A. Approved for public release: distribution unlimited.

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

This research paper uses a problem/solution framework to identify how Air Force Space Command (AFSPC) can integrate and improve cybersecurity for legacy and modern weapon systems to reduce the cybersecurity attack-surface. With Department of Defense (DOD) networks and mission systems undergoing nearly 250,000 attacks a day, AFSPC must take immediate action to thwart the attacks from adversarial nation states and non-state actors alike. While there are numerous cybersecurity concerns, or non-compliant cybersecurity controls across all weapon systems, not all non-compliant controls contribute equally to the cyber-attack surface and overall vulnerability of weapon systems. For this reason, the major contributors or key issues surrounding the current cybersecurity attack-surface have been identified as policy, defense-in-depth, threat intelligence, and the DOD mandated transition from the DOD Information Assurance Certification and Accreditation Process to Risk Management Framework (RMF). Utilizing RMF and the National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity three alternative solutions are evaluated to identify the best option for AFSPC to systematically implement to reduce the overall cybersecurity attack-surface for its modern and legacy weapon systems.

SECTION 1: INTRODUCTION

Securing AFSPC weapon systems through cybersecurity is necessary to maintain the advantage to the United States (US) and its warfighters as both nation-states and non-state actors are developing new capabilities that threaten US ability to fly, fight, and win in air, space, and cyberspace. As the lead command for space and cyberspace, AFSPC understands that cyberspace spans the air, land, sea, and space domains and integrates AFSPC weapon systems to give the US an advantage at war and peace and therefore cyberspace mission systems must be secured from adversarial attack.

DOD networks and mission systems undergo 250,000 cyber-attacks every day and Secretary of Defense, Ashton Carter, warned that the cyber threat to mission systems "is increasing in severity and sophistication" and "it comes from state and non-state actors alike."[1] Many critics argue that securing weapon systems is expensive, difficult, and a never ending loop of Observe, Orient, Decide, and Act that delivers minimal results with no measurable proof that security mitigations and resolutions are effective or even warranted. The threat is real and ongoing as indicated by *The National Strategy to Secure Cyberspace* and associated weapon systems which highlights three strategic priorities. First, to prevent cyber-attacks against America's critical infrastructure.[2] This first step is essential to protecting both legacy and modern weapon systems as part of a defense-in-depth. Second, US national policy seeks to reduce national vulnerability to attacks that would reduce the overall attack surface which means to reduce the amount of vulnerabilities and adversary can exploit on the mission system.[3] Finally, and most essential, is minimizing damage and recovery time from cyber-attacks as no system is one hundred percent secure and will never be impenetrable.[4]

This research paper utilizes the problem/solution framework to identify how AFSPC can integrate and improve cybersecurity for legacy and modern weapon systems to reduce the cybersecurity attack surface within the current fiscal environment given the DOD mandated use of the RMF beginning 1 October 2016. By identifying the primary issues and concerns contributing to the cyber-attack surface, alternative solutions can be developed and implemented to significantly reduce the cybersecurity attack surface within this fiscally constrained environment effecting the DOD and AFSPC.

Because of the ongoing adversarial attacks on DOD networks and mission systems this research paper will explore options to reduce the cyber-attack surface for AFSPC systems by partnering DOD and industry to provide defense-in-depth regarding mitigation or resolution of the most critical non-compliant cybersecurity controls that are both mission system specific and enterprise wide solutions. Additional options to reduce the cybersecurity attack-surface must include continuous monitoring at the tactical and operation level and identifying a way to inform cybersecurity professionals when the real-time threat has increased. Only then will AFSPC mission systems be flexible enough to adjust to the ever changing cyber threat landscape to identify, protect, detect, respond, and recover to cyber threats in real-time.

SECTION 2: DESCRIPTION OF THE PROBLEM AND ITS KEY ISSUES

While the Department of Defense does have an overall Cyber Strategy to “guide the development of its cyber forces and strengthen US cyber defense and cyber deterrence posture” to defend networks, national interests, and cyber support to military operational and contingency plans, it is too slow in the making.[5] For instance, the cyber mission force goal for 2018 is to have approximately 130 teams that are delineated to support either National Mission Teams, Cyber Protection Teams, Combat Mission Teams, or Support Teams.[6] AFSPC can ill afford to wait until more cyber mission teams are trained and stood up defend its mission systems and must take measures now to ensure the warfighter can continue to fly, fight, and win in space and cyberspace.

AFSPC has over two hundred major weapon systems that span six primary capabilities to provide support to all DOD warfighters. These capabilities include Missile Warning / Missile Defense, Situational Awareness / Command and Control, Military Satellite Communications, Launch and Test Range Systems, Precision, Navigational and Timing, and Air Force Satellite Control Station to support Combatant Commanders. Many of these systems are considered legacy weapon system that were developed prior to any cyber-attack concerns and therefore do not have cybersecurity built into the weapon system and requires some form of cybersecurity being bolted onto the weapon system in attempt to secure the system. These legacy weapon systems include early warning radars, satellite ground control stations and launch and test range systems that have operated since the late 1960s and early 1970s. Additionally, within the six primary mission capabilities provided by AFSPC to support Combatant Commanders and the warfighters are modern weapons systems. These modern weapon systems have included some cybersecurity measures beginning in the acquisition period by building in cybersecurity based on both the DOD Information Assurance Certification and Accreditation Process from 2000 to 2015 and the RMF. AFSPC modern weapon systems include newly developed operation and data collection centers, modifications to satellites and ground stations, and major legacy system upgrades within the past 10 years.

To reduce the cyber-attack surface, AFSPC must zero in on the primary issues and concerns that are major contributors to the current cyber-attack surface for legacy and modern weapon systems.   While there are numerous cybersecurity concerns, or non-compliant cybersecurity controls across all weapon systems, not all non-compliant controls contribute equally to the cyber-attack surface and overall vulnerability of the weapon system. For this reason, the major contributors or key issues surrounding the current cybersecurity attack-surface have been identified as policy, defense-in-depth, threat intelligence, and the DOD mandated transition to RMF for AFSPC weapon systems.

Policy

Policy for cybersecurity is either overwhelming or absent depending on the subject and is covered by a wide range of documentation that includes DOD directives, DOD instructions, DOD manuals, joint publications, NIST special publications, chairman joint chiefs of staff instructions, committee on national security systems instructions, federal information processing standards, homeland security presidential directive - 12, and executive orders. According to figure 1, Defense Information Systems Agency has identified over 150 cybersecurity related policies and issuances such policies and directives developed by the DOD Deputy Chief Information Officer for cybersecurity.[7] To add to the confusion, these 150 plus policies and issuances are developed by several organizations that include the DOD, Joint Chiefs of Staff, National Information Assurance Partnership, Director of National Intelligence, National Security

Agency, United States Strategic Command, and the Under Secretary of Defense for Acquisition, Technology, and Logistics, Comptroller, Intelligence, Policy, and Personnel and Readiness to name a few. To further complicate the policy picture, the 150 plus policies are segregated into four broad categories (i.e., Organize, Enable, Anticipate and Prepare) that do not align with the DOD mandated RMF six major categories of Categorize, Select, Implement, Assess, Authorize, and Monitor which was implemented on 1 October 2016. In fact, according to the DOD Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, "cybersecurity requirements for DOD information technologies will be managed through the RMF consistent with the principles established in the NIST which are the six steps of RMF."[8]

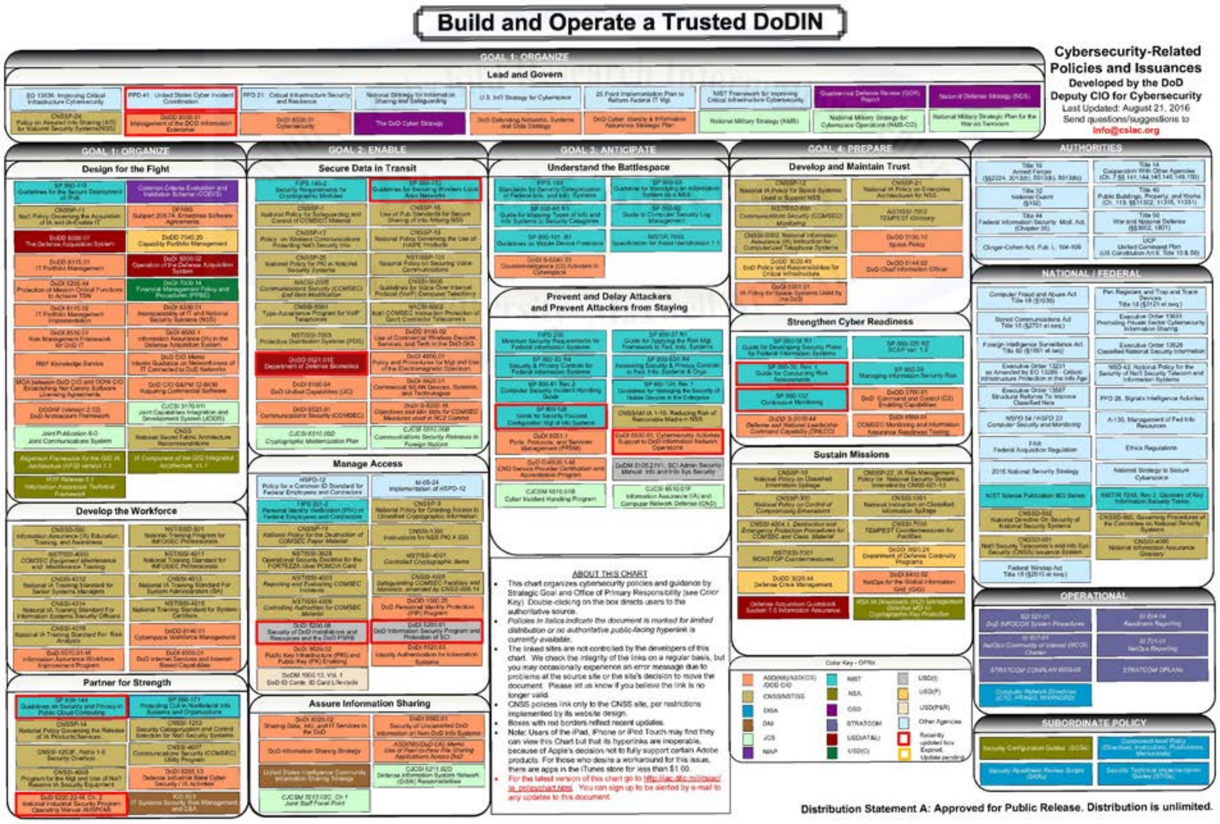

Build and Operate a Trusted DoDIN
Cybersecurity-Related Policies and Issuances Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: August 21, 2016
Send questions/suggestions to info@cslac.org
GOAL 1: ORGANIZE
Lead and Govern
Design for the Fight
Develop the Workforce
Partner for Strength
GOAL 2: ENABLE
Secure Data in Transit
Manage Access
Assure Information Sharing
GOAL 3: ANTICIPATE
Understand the Battlespace
Prevent and Delay Attackers and Prevent Attackers from Staying
ABOUT THIS CHART
GOAL 4: PREPARE
Develop and Maintain Trust
Strengthen Cyber Readiness
Sustain Missions
Color Key - OPRs
AUTHORITIES
NATIONAL / FEDERAL
OPERATIONAL
SUBORDINATE POLICY
Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Figure 1. Build and Operate a Trusted DOD Information Network

On the other hand, there is no specific guidance on how to conduct continuous monitoring for mission systems or any DOD Information Technology system for that matter. While DOD instruction 8510.01 states that "continuous monitoring capabilities will be implemented to the greatest extent possible," it does not define continuous monitoring since the last incorporated change on 24 May 2016 which is problematic as monitoring is the sixth and final step of RMF and is required to maintain a continuous authority to operate at a risk level accepted by the Authorizing Official.[9] Additionally, there are a total of 14 RMF cybersecurity controls that apply to continuous monitoring and are identified as procedures under the security assessment and authorization category within the NIST Special Publication 800-53Ar4.[10] Unfortunately, the Defense Information Systems Agency knowledge Service authoritative website for all RMF controls and procedures states that these procedures are currently awaiting "future DOD-wide continuous monitoring guidance to be published" which has been the status since March 2014.[11]

Defense-in-Depth

By not defining DOD-wide continuous monitoring guidance, the DOD has left the operational, tactical, and strategic levels within AFSPC to decide what constitutes cybersecurity defense-in-depth. This is not to say that physical measures such as gates, guards, and guns are not utilized to support the weapon system security or that firewalls and cross domain solutions are not in place in effort to keep the external threat at bay. Some AFSPC legacy and modern weapon systems have pointed to the Chairman Joint Chiefs of Staff Instruction 6510.01F and attempted to create a Tier 3 computer network defense environment to continuously monitor their system from an operational standpoint. But what some call continuous monitoring is nothing more than audit logs may or may not be reviewed by the cybersecurity team while others have leaned forward to make a concerted effort to monitory 24/7 and review logs daily, but even this is not real-time continuous monitoring. Additionally, the Combatant Commander has failed to follow CJCSI 6510.01F as they have not established Tier 2 computer network defense services or “obtained Tier 2 computer network defense support from the Defense Information Systems Agency or other US Strategic Command (USSTRATACOM) accredited Tier 2 service provider to coordinate and direct protective measures and implement DOD-wide operational and defensive direction from USSTRATCOM.”[12] This means that even if the tactical or field level has instituted some form of Tier 3 computer network defense service provider, there is no operational level or Tier 2 service provider to report suspicious behavior, anomalies, or evidence of internal or external actions that compromise the mission system. Furthermore, without a Tier II computer network defense service provider established, the strategic level, or in this case Cyber Command Tier I service provider, does not receive any information from the tactical or operational level service providers to coordinate and direct protective measures. Simply put, if mission systems were equivalent to our homes, all mission systems have street lights, locked doors, locked windows, and the occasional dog to deter the bad guy, but do not have an ADT or police on standby if their home grown alarm system alerts the homeowner of an intruder.

Threat Intelligence

According to Shon Harris, author of the *Certified Information System Security Professional*, risk to an Information Technology system, or in this case an AFSPC mission system, is determined by identifying the threats, vulnerabilities, asset value, and control gaps to obtain the residual risk.[13] Once threats, vulnerabilities, asset value, and control gaps are identified the residual risk is calculated as (threats x vulnerability x asset value) x control gaps = residual risk. Identifying residual risk starts in the field with the information system security manager and the security team for a specific mission system (i.e., 1 of ~250 AFSPC mission systems) and is then presented to the security control assessor representative for an independent evaluation of residual risk. Once the security control assessor representative completes his/her assessment, the residual risk is presented to the security control assessor who reviews all non-compliant controls and makes a recommendation to the authorizing official for an authorization decision of authority to operate or denial of authority to operate.[14]

According to DOD instruction 8510.01, the security control assessor has the responsibility to conduct a risk assessment on all non-compliant controls and consider, at a minimum, the following factors in producing a risk level; (1) determine that a “credible or validated threat source and potential event exists that is capable of, and likely to, exploit vulnerabilities in the implementation of the control,” (2) estimate of adequacy of existing “mitigations provided by the hosting enclave, computer network defense service provider or other protective measures,” (3) the “cybersecurity attribute and associated categorization impact level to the control,” and (4) “estimate of impact of a successful threat event.”[15] All of these risk assessment steps are accomplished today without knowing the specific threat to an AFSPC mission system. While most cybersecurity personnel carry either a Secret or Top Secret security clearance they are not privy to the special access program or higher level threat information. Without specific threat information the residual risk formula will not be accurate and may actually be watered down to the lowest level where every non-compliant control becomes a Category III vulnerability or elevated to the highest level and every non-compliant control becomes a Category I vulnerability. A lack of confidence in the residual risk determination, due to inaccessibility to specific threat information, leaves program managers with the problem of which vulnerabilities of possibly hundreds of non-compliant controls to resolve or mitigate first.

Risk Management Framework Transition

On 12 March 2014 the DOD chief information officer directed the "Office of the Secretary of Defense, Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DOD Field Activities, and all other organizational entities within the DOD" to transition from the DOD information assurance certification and accreditation process to the RMF within six months. Based on feedback from the field the DOD chief I\information officer retracted the original date of transition and set 1 October 2016 as the new transition deadline.[16] RMF has both positive and negative effect on assessing risk across AFSPC mission systems. Some of the positives include; (1) cybersecurity controls that are more granular in nature reducing the amount of interpretation by the cybersecurity teams, (2) five risk levels ranging from very low, low, moderate, high, and very high vice three risk levels in DOD information assurance certification and accreditation process, (3) aligns with industry standards to enable reciprocity with industry, and (4) risk level driven vice checklist drive. On the other hand, the negatives of RMF include; (1) the number of cybersecurity controls that must be reviewed and (2) based on continuous monitoring and acceptable risk levels vice checklist driven and continuous authority to operate issuances.

The primary negative of RMF is the sheer number of cybersecurity controls that must be reviewed which increases from 110 to approximately 1,000 under RMF and will require a considerable amount of time to review. According to figure 2, RMF consists of six steps in which five of the six steps involve selecting, implementing, assessing, authorizing, and monitoring the nearly 1,000 cybersecurity controls.[17] With the residual risk remaining

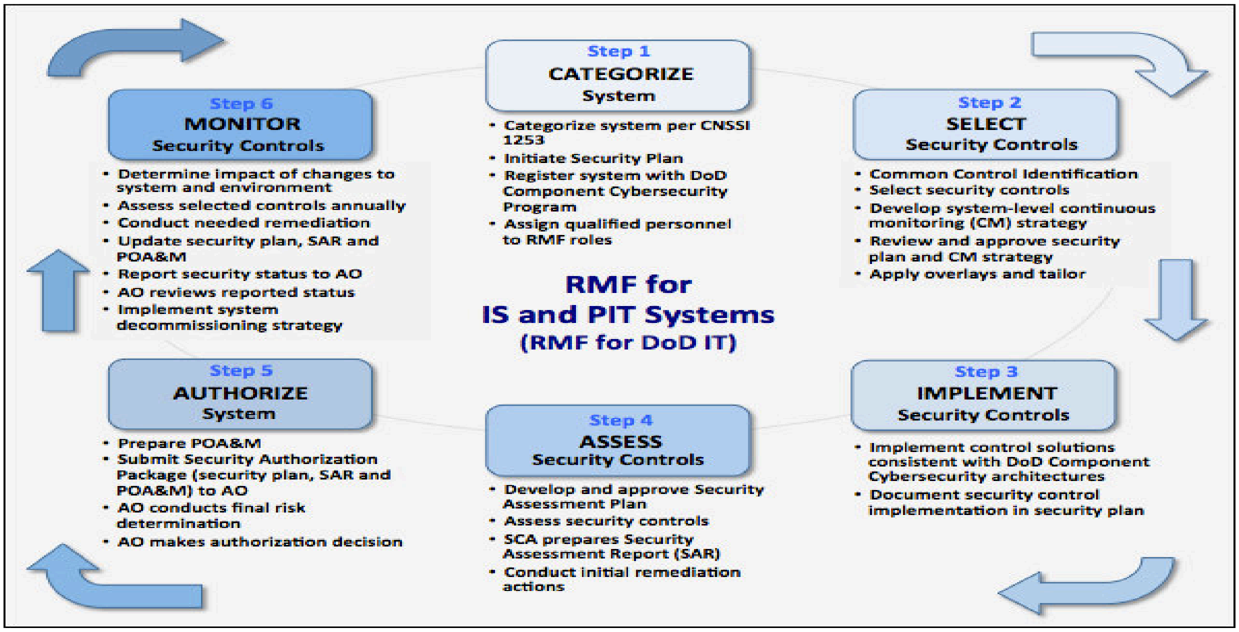

Step 1
CATEGORIZE
System
• Categorize system per CNSSI 1253
• Initiate Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring (CM) strategy
• Review and approve security plan and CM strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in security plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare POA&M
• Submit Security Authorization Package (security plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF for
IS and PIT Systems
(RMF for DoD IT)

Figure 2. RMF for Information Systems and Platform Information Technology Systems

relatively the same, the number of non-compliant controls receiving a Categorization level of I, II, or III will multiply tenfold due to the granular nature of RMF. This leaves Program Managers and the cybersecurity team with the daunting task of deciding which non-compliant controls they should work towards mitigating or resolving. Obviously they will start with the non-compliant Category I controls first, but after fixing or mitigating all of the Category I controls the sheer number of non-compliant Category II controls, based on first-hand experience, has averaged in the hundreds for AFSPC legacy systems and nearly as high for modern systems. The approach to resolving or mitigating the overwhelming number of non-compliant Category II controls varies from considering the insider threat first and resolving those vulnerabilities or considering the external threat first to identify and fix those findings across all AFSPC mission systems.

SECTION 3: DESCRIPTION OF WHAT IS BEING MEASURED

To measure risk across a weapon system each of the nearly 1,000 cybersecurity controls, objectives, and attributes under RMF must be assessed to identify whether the mission system is either compliant, non-compliant, or not applicable for each of attributes, objectives and controls. Once this is accomplished, the non-compliant controls, objectives and attributes must undergo a process to identify the likelihood and impact of a threat event initiation and occurrence by using NIST, Special Publication 800-30 as a guideline. NIST 800-30 is the guide for conducting risk assessments and was developed by NIST along with other federal agencies and offices as well as the private sector to improve information security by complementing existing standards and guidelines employed for the protection of national security systems. The first step to determining the risk of a non-compliant control to a mission system is to determine the likelihood of occurrence by using assessment scales as a starting point. Utilizing available intelligence data, the cybersecurity team must determine the likelihood of external or internal adversarial threat event initiation and assign it a qualitative value that ranges from very low, low, moderate, high, and very high. This qualitative value is selected based on the descriptions in table one which describes the likelihood that an adversary will initiate the threat event and range from almost certain, highly, likely, somewhat likely, unlikely and highly unlikely.[18] In addition to calculating the likelihood of an adversarial threat event, the cybersecurity team must consider the likelihood of a threat event occurrence that is non-adversarial such as human error, human accident, or acts of nature that can be just as destructive as an adversary attack. By researching tactics, techniques, procedures, and historical acts of nature, the cybersecurity team then

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table 1. Assessment Scale-Likelihood of Threat Event Initiation (Adversarial)

determine the likelihood and qualitative value of a non-adversarial threat event occurrence based on the descriptions provided in table two which ranges from almost certain to highly unlikely and quantifies the occurrence likelihood by stating the amount of times the non-adversarial act is likely to occur each year or less than once every 10 years.[19]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur, or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur, or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur, or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur, or occurs **less than once every 10 years**.

Table 2. Assessment Scale-Likelihood of Threat Event Occurrence (Non-Adversarial)

With the likelihood of the adversarial and non-adversarial threat event initiation and occurrence qualitatively captured, for the non-compliant control, the next step is to qualitatively capture the likelihood of the threat event resulting in an adverse impact to the mission system. To accomplish this task the cybersecurity professionals must determine the level of impact to the mission system when the threat event is initiated or occurs by reviewing the descriptions in table three and assigning a qualitative value from an impact standpoint.[20] Once the likelihood of the event initiation or occurrence is captured for both the adversarial and non-adversarial threats along with the level of impact to the mission system when the threat occurs the next step is to capture the overall likelihood by plotting the qualitative values captured in tables one through three. For instance, if the qualitative value from the adversarial threat event initiation is High and the qualitative value from the non-adversarial threat occurrence is Moderate, the likelihood of threat event initiation or occurrence in table four would be High as this is the highest

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Table 3. Assessment Scale-Likelihood of Threat Event Resulting in Adverse Impacts

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Results in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 4. Assessment Scale-Overall Likelihood

qualitative value of the two and if the qualitative value impact was Very High, then the overall likelihood would be plotted as Very High for the non-compliant control as depicted in table four.[21] Once the overall likelihood is captured; the next step is to determine the impact of threat events to obtain the qualitative value that will aid in determining the risk level for the non-compliant control. These threat events are described in table five as either multiple severe or catastrophic, severe or catastrophic, serious, limited, or negligible which range from very high to very low.[22]

Qualitative Values	**Semi-Quantitative Values**		**Description**
Very High	96-100	10	The Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organization, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. The threat event might cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. The threat event might cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.
Low	5-20	2	The threat could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. The threat event might cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary function, but the effectiveness of the function is noticeably reduced.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations; organization assets, individuals other organizations, or the Nation.

Table 5. Assessment Scale-Impact of Threat Events

Finally, with the likelihood and impact qualitatively captured, the cybersecurity team identifies the level of risk for the non-compliant control by first plotting the likelihood of the threat event occurrence that resulted in the adverse impact and the plotting the qualitative impact of threat events captured in table five. For instance, if the overall likelihood in table four was Very High and the impact of threat event in table five was determined to be High, then the overall level of risk for the non-compliant control would be High as depicted in table six.[23]

Likelihood of (Threat Event Occurs and Results in Adverse Impact	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

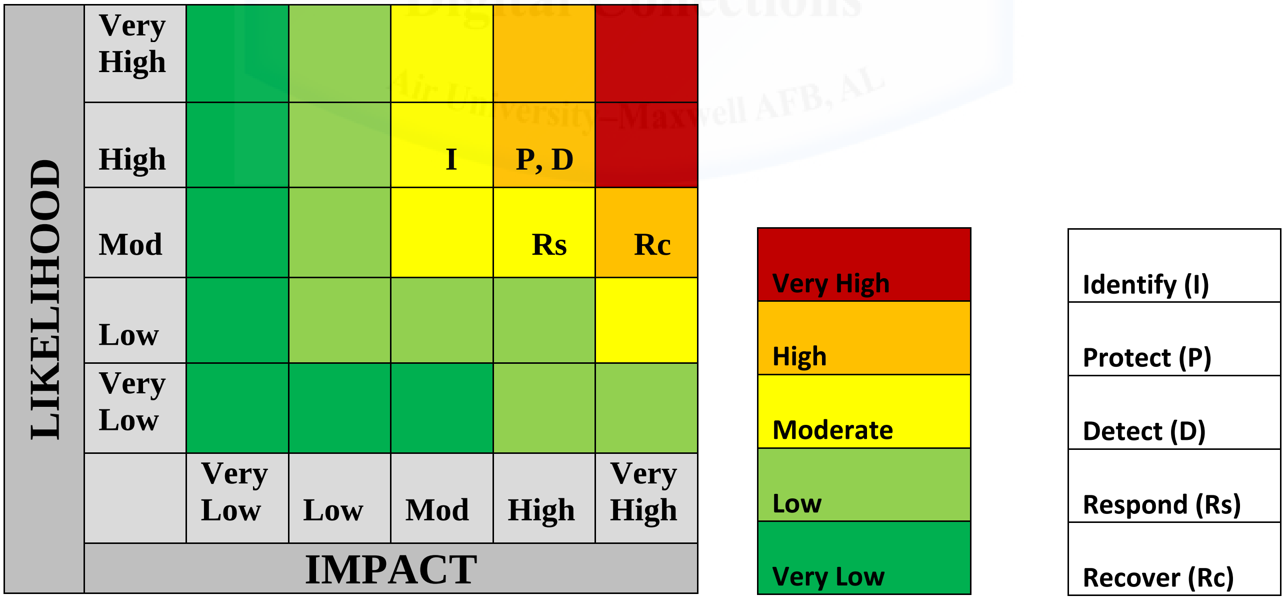
Table 6. Assessment Scale-Level of Risk (Combination of Likelihood and Impact)

Plotting the risk is not enough, cybersecurity professionals must relay the risk to leadership and develop a plan of action to mitigate and resolve all critical non-compliant controls starting with the highest risk level. To relay the risk to leadership, NIST 800-30 has described all five risk levels as shown in table seven.[24]

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very High risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 7. Assessment Scale-Level of Risk

The difficulty comes when plotting eighteen families of controls and nearly 1,000 objectives and attributes into a 5x5 cybersecurity risk matrix, or any other report, that is both understandable and capable of relaying the appropriate information required to reduce the overall risk of mission systems. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, directed the NIST to "include a set of standards, methodologies, procedures, and processes that align policy, business, and technology approaches to address cyber risk."[25] Subsequently, NIST developed the Framework for Improving Critical Infrastructure Cybersecurity which enabled organizations to better understand and mold its cybersecurity program using the functions of Identify, Protect, Detect, Respond and Recover (IPDRR) with the DOD mandated RMF. This framework defines the five functions as; (1) Identify - "develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities," (2) Protect - "develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services," (3) Detect - "develop and implement the appropriate activities to identify the occurrence of a cybersecurity event," (4) Respond - " develop and implement the appropriate activities to take action regarding a detected cybersecurity event," and (5) Recover – "develop and implement the appropriate activities to maintain plans for resilience."[26] By grouping the eighteen control families and nearly a 1,000 objectives and attributes into IPDRR, the cybersecurity team can apply the principles and best practices of RMF to improve the security of critical infrastructure and present management and leadership with a an accurate and easily understood risk picture. For instance, the NIST 800-30 level of risk identified in table six can be modified into an operational 5x5 risk matrix and the high water mark for each non-compliant control, objective and attribute can be plotted using IPDRR as shown in table eight.



LIKELIHOOD	Very High	🟢	🟩	🟨	🟧	🟥
	High	🟢	🟩	🟨 I	🟨 P, D	🟥
	Mod	🟢	🟩	🟨	🟨 Rs	🟧 Rc
	Low	🟢	🟩	🟩	🟩	🟨
	Very Low	🟢	🟢	🟢	🟩	🟩
		Very Low	Low	Mod	High	Very High
		IMPACT				

🟥 Very High
🟧 High
🟨 Moderate
🟩 Low
🟢 Very Low

Identify (I)
Protect (P)
Detect (D)
Respond (Rs)
Recover (Rc)

Table 8. Assessment Scale-Level of Risk 5x5 (Combination of Likelihood and Impact)

To address the four primary issues/concerns of policy, defense-in-depth, threat intelligence, and RMF transition, each of the RMF attributes, objectives, and controls must be aligned to the five functions described by NIST 800-30. Table nine aligns the primary

Functions	RMF Control Families	RMF Procedure	Primary Issue/Concern
IDENTIFY	Program Mgt (PM)	N/A	**Policy** = Continuous Monitoring is not defined by the DoD. Implementation guidance states automated mechanisms to detect the presence of unauthorized components within the information system continuously. **Threat Intelligence** = Unavailable or too broad to perform risk assessment. Implementation guidance states threat analyses for the as-built, system component, or service and defines the breadth of threat modeling and vulnerability analysis to be performed by developers for the information system.
	System & Services Acquisition (SA)	SA-4(8).1, SA-4(8).2, SA-11(2).1, & SA-15(4).1	
	Identification & Authentication (IA)	N/A	
	Risk Assessment (RA)	N/A	
	Configuration Management (CM)	CM-8(3).2 & CM=8(3).4	
PROTECT	Access Control (AC)	N/A	**Policy** = Continuous Monitoring is not defined by the DoD. Implementation guidance states future DoD-wide CM guidance to be published.
	Awareness & Trng (AT)	N/A	
	Media Protection (MP)	N/A	
	Security Assessment & Authorization (CA)	CA-7.1 to 7.11, CA-7(1), & CA 7(1).2	
	Maintenance (MA)	N/A	
	Personnel Security (PS)	N/A	
DETECT	Audit/Accountability (AU)	N/A	**Defense-in-Depth** = Tier II CSSP not established for AFSPC weapon systems. Implementation guidance states CSSP Tier 1 will pass the information to the accredited Tier 2 CSSPs. Tier 2 CSSPs are responsible for ensuring all Tier 3 entities receive information.
	System & Integrity (SI)	SI-2(2).1, SI-2(2).2, & SI-5.7	
	System & Communication Protection (SC)	SC-7(13).1 & SC-7(13).2	
RESPOND	Incident Response (IR)	IR-4.1, IR-7(2).1, & IR-7(2).2	**Defense-in-Depth =** Tier II CSSP not established for AFSPC weapon systems. Implementation guidance states “the organization must establish a formal agreement with a cybersecurity service provider (CSSP).
RECOVER	Planning (PL)	CP-4(4)	**RMF Transition =** RMF brings nearly 10 times the scrutiny via controls which results in 10 times the number of non-compliant controls. Implementation guidance states a full recovery of information system and philosophy, requirements, and approach to be taken with regard to confidentiality, integrity, and availability for the organization.
	Contingency Planning (CP)	Pl-8	

Table 9. Map Primary Concerns and RMF Controls to NIST Functions

issues/concerns for AFSPC modern and legacy weapon systems, identifies the subsequent RMF procedures (attributes and objectives), aligns the procedures with the RMF control family, and then aligns the RMF control family with the one of the 5 functions identified by NIST. The DOD mandated RMF process coupled with the NIST 800-30 IPDRR response to Executive Order 13636 and the 5x5 assessment scale level of risk (table eight) will be utilized to analyze the alternatives solutions to identify a recommendation for AFSPC to reduce the cybersecurity attack surface for modern and legacy weapon system in regards to policy, defense-in-depth, threat intelligence, and the RMF transition.

SECTION 4: DISCUSSION OF ALTERNATIVES

With a clear understanding of how RMF and NIST 800-30 assesses risk of non-compliant controls, objectives, and attributes the stage is set to discuss courses of action (COAs) to reduce the cybersecurity attack surface for AFSPC mission systems. A total of three COAs will be presented and range from status quo or continue to operate within the current cybersecurity attack surface, to an AFSPC solution to mitigate or resolve the four primary issues/concerns, and finally a DOD solution that addresses the four primary issues from and enterprise-wide standpoint.

COA 1: Status Quo - Today

The first COA, status quo, is a viable option for critics who argue that securing weapon systems is expensive, difficult, and a never ending observe, orient, decide, and act loop that delivers minimal results with no measurable proof that security mitigations and resolutions are effective or even warranted. Under this COA, AFSPC will continue to operate approximately 250 mission systems across six primary capabilities to support the warfighter without reducing the cybersecurity attack surface. AFPSC will continue to wait on the DOD to define continuous monitoring and provide specific guidance to the fourteen RMF security controls that have been awaiting future DOD-wide guidance to be published since March 2014. Additionally, AFSPC mission systems will continue to operate without a Tier II cyber security service provider (CSSP) to provide defense-in-depth both down to the tactical level and up to the strategic level to report suspicious behavior, anomalies, or evidence of internal or external actions that not only compromises the mission system but compromise the AFSPC mission. Furthermore, specific threat intelligence for AFSPC systems will remain unavailable and the risk calculated by cybersecurity professionals will be nothing more than a guess as threat is a major inject to the formula to determine residual risk. This leaves the cybersecurity team to caution on the high side for threat which drives the number of non-compliant controls up and elevates the risk to either high or very high. Finally, without specific threat data and given the number of controls in RMF, Program Managers for the weapon systems will have no clear path on which of the non-compliant controls to resolve or mitigate first.

COA 2: AFSPC Solution – Short to Mid-Term

The AFSPC COA presents partial solutions to the four primary issues/concerns to address the absence of policy for continuous monitoring, the lack of defense-in-depth across all mission systems, the absence of specific threat intelligence to mission systems, and the number of non-compliant controls under RMF. First, AFPSC must update AFSPCI 33-202, *Information Assurance,* to define continuous monitoring as a Tier III CSSP and mandate AFSPC communication squadrons act as the Tier III CSSPs in support of the mission systems supporting the six primary capabilities vice sustainers of the Air Force non-secure internet protocol router network and secret internet protocol router network. To accomplish this, communication squadrons must be realigned under the Operations Group, be repurposed as defensive cyber operators, and receive the necessary training to perform 24/7 hands on monitoring and reporting of unauthorized components within the weapon system to a Tier II CSSP. Second, AFSPC must address the lack of defense-in-depth when it comes to a Tier II CSSP.

AFSPC must financially resource and provide the personnel to stand up a MAJCOM-wide Tier II CSSP for all mission systems. Today, the 24th Air Force provides Tier II CSSP support for both non-secure and secret network but not for any of the nearly 250 spaced based mission systems. The MAJCOM-wide Tier II CSSP should be managed by the 14th Air Force by utilizing existing space based infrastructure such as the Air Force satellite control network and the space command digital integrated network which are already managed by the 14th Air Force and essentially act as the non-secure and secret network for space systems. With the policy and defense-in-depth concerns addressed it is time to tackle the absence of specific threat intelligence for AFSPC mission systems.

AFSPC must task the Intelligence Directorate to research and provide specific threat information to the cybersecurity teams in the field who develop, acquire, sustain, and modify mission systems and to the cybersecurity teams in the Headquarters who review and assess risk on behalf of the authorizing official who must review the overall risk of the system and grant authority to operate. The problem arises when the threat data is classified at a level that is above Top Secret and requires special access program which most cybersecurity experts do not have and therefore are not privy to the threat information which is a major factor in assessing residual risk. The simple answer is to evaluate all cybersecurity risk assessors for the highest clearance level possible, but due to cost, time, and a trend to reduce eligible (in access) clearances by 2.1% for a total 62,074 less clearances from FY14 to FY15 this is not possible.[27] Therefore, AFSPC must institute a Cyber Condition (CYBERCON) program with specific steps for cybersecurity teams to initiate based on the threat level known by the intelligence community. When the AFSPC intelligence community increases the CYBERCON (scale of 1 to 5) cybersecurity professionals will take additional security precautions such as disconnecting from a cleared defense contractor facilities, or locking down non mission essential ports, or increasing the manual review of audit logs for anomalies. CYBERCON will be the cyber equivalent of Force Protection Condition (FPCON) and the condition will change with the threat to AFSPC systems. The final AFSPC concern/issue deals with the sheer number of RMF controls and how to prioritize the non-compliant controls for resolution or mitigation actions.

The DOD mandated transition from DOD information assurance certification and accreditation process to RMF in March of 2014 with an effective date of 1 October 2016. This transition multiplied the number of controls tenfold which subsequently multiplied the number of non-compliant controls tenfold due to the granular nature of RMF. With potentially hundreds of non-compliant controls to resolve or mitigate a Program Manager and cybersecurity team will concentrate on the very high non-compliant controls first, and then the high non-compliant controls and so on. The problem arises with the number of moderate non-compliant controls for modern and legacy weapon systems that can number in the hundreds. AFSPC must look to the System Administration, Networking, and Security (SANS) Institute which was established in 1989 as a cooperative research and education organization and is the most trusted and largest source of information security training and security certification in the world.[28] AFSPC can leverage SANS work on capturing critical security controls for effective cyber defense that will provide specific and actionable ways to stop today's most pervasive and dangerous attacks. The critical security control list was created by the National Security Agency red and blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's leading forensics and incident response teams.[29] By implementing critical security controls, AFSPC can concentrate its limited monetary budget towards implementing controls that pay the highest dividend to defend legacy and modern weapon systems.

COA 3: DOD Enterprise-Wide Solution – Mid to Long-Term

The DOD COA presents enterprise-wide solutions to the four primary issues/concerns to address the lack of policy for continuous monitoring, the absence of defense-in-depth across all mission systems, the lack of specific threat intelligence to mission systems, and the number of non-compliant controls under RMF. This COA closely resembles the actions AFSPC must take in COA 2, but elevates the actions up to DOD level for consolidation and enterprise-wide solutions to the growing cybersecurity threat. First, the DOD must take a hard look at all the cybersecurity regulations, policies, directives, instructions, etc., (Figure 1) and consolidate and/or reduce the number of policies and align all remaining policies under the six steps of RMF (Figure 2). In addition, the DOD must utilize working groups such as the task force cyber secure working group to once and for all define continuous monitoring and update the necessary directives for the tactical, operational, and strategic level CSSPs to work together to secure the AFSPC and DOD mission systems through reciprocity. Secondly, the DOD must address the lack of defense-in-depth when it comes to Tier II CSSPs.

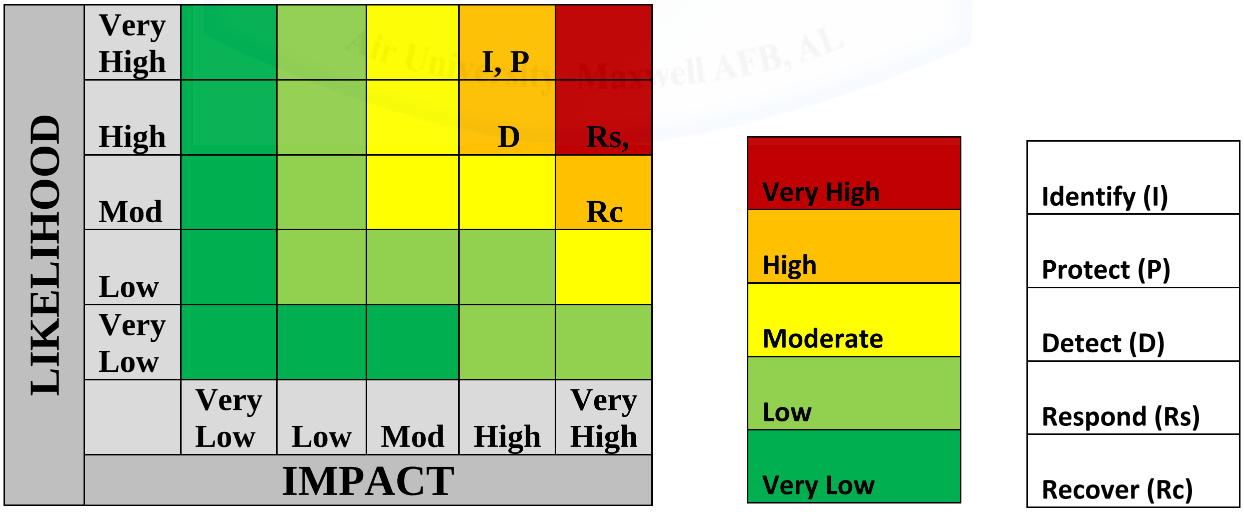
The DOD must consider Joint Tier II CSSPs where it makes sense. For instance, USSTRATCOM is the authorizing official and component chief information officer for the nuclear, command, control, and communication mission which spans AFSPC, the Navy, NORAD NORTHCOM, and Air Force Global Strike Command. In this case, the DOD must resource USSTRATCOM to standup a Joint Tier II CSSP to reduce the cybersecurity attack surface across all nuclear, command, control, and communication systems in the DOD portfolio. To accomplish this, the DOD must look at mission systems from a capability standpoint and stand up Joint Tier II CSSPs based on mission system functionality and location and man the CSSPs with Airmen, Soldiers, Seaman, Marines, Civilians, and Contractor expert.   Finally, to ensure defense-in-depth remains strong and has the best personnel available the DOD must manage military career assignments that traverse Tier III, II, and I CSSPs across all services and pay bonuses equal to civilian and contractor counterparts.

In regards to the lack of threat intelligence for specific mission systems, the DOD must utilize the National Security Agency and other intelligence organizations to capture the real-time threat and relay the threat via a DOD-wide CYBERCON. The DOD must establish specific steps to take during each level of CYBERCON and make the steps specific to the mission systems such as aircraft, ships, submarines, satellites, and field artillery. With a DOD-wide CYBERCON, AFSPC and all other MAJCOMS throughout all services will benefit and lock down their mission systems as the threat increases and essentially stop the threat from moving laterally across mission systems that are interoperable. Finally, the DOD must take a look at all RMF controls and develop a zero tolerance list for non-compliant controls.

By utilizing the SANS work on critical security controls the DOD must create a zero tolerance critical RMF control list that must be compliant if applicable to the mission system. The RMF controls, objectives, and attributes that number nearly 1,000 must be scaled down based on the SANS critical security controls work to the most important 100 controls and if non-compliant, the Program Manager must escalate the non-compliance up to their component and DOD chief information officers with a get well date or a request for funding to resolve the critical non-compliant control. By using the SANS work on critical security controls, identifying the most critical 100 RMF controls the DOD can concentrate its limited monetary budget towards implementing controls that pay the highest dividend to defend mission systems.

SECTION 5: RESULTS OF COMPARISONS BETWEEN ALTERNATIVE SOLUTIONS

To compare the three COAs the mandated RMF process, NIST 800-30 process of Identify, Protect, Detect, Respond and Recover (IPDRR), and the 5x5 assessment scale level of risk will be utilized to analyze the alternative solutions to recommend the best option to reduce the cybersecurity risk for AFSPC mission systems. First, a risk level foundation must be set in regards to a typical AFSPC mission system for the areas of IPDRR that align to the RMF controls, attributes, and objects and the four primary issues/concerns with all legacy and modern AFSPC mission systems. Therefore, figure nine identifies the foundation starting point for AFSPC mission systems that do not practice continuous monitoring due to the lack of DOD policy (Identify and Protect), the absence of defense-in-depth such as a Tier II Cybersecurity Service Provider (Detect and Respond), the inability to identify the true threat to mission systems based on lack of intelligence information or security clearance (Identify), and finally no clear guidance on which of the non-compliant controls, attributes, and objectives a cybersecurity team



LIKELIHOOD						
	Very High	🟩	🟢	🟨	🟧 I, P	🟥
	High	🟩	🟢	🟨	🟧 D	🟥 Rs,
	Mod	🟩	🟢	🟨	🟨	🟧 Rc
	Low	🟩	🟢	🟢	🟢	🟨
	Very Low	🟩	🟩	🟩	🟢	🟢
		Very Low	Low	Mod	High	Very High
	IMPACT					

🟥	Very High
🟧	High
🟨	Moderate
🟢	Low
🟩	Very Low

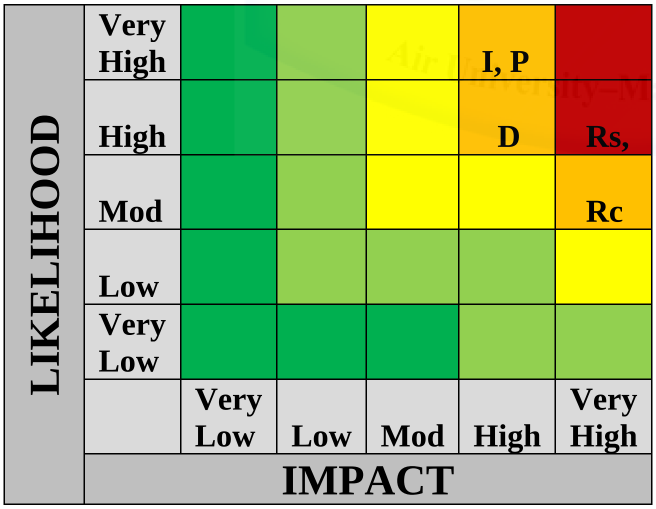
Identify (I)
Protect (P)
Detect (D)
Respond (Rs)
Recover (Rc)

Table 10. Risk Assessment Baseline

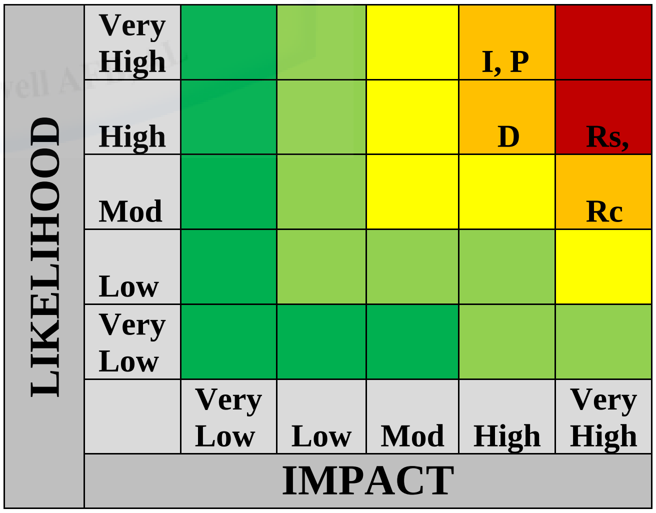
should resolve or mitigate first when there are potentially hundreds of non-compliant controls (Recover). This foundational baseline is not specifically related to any one AFSPC mission system risk level but is a typical RMF raw rating risk and NIST 800-30 plotting against each of the RMF controls identified in table nine.

COA 1 Comparison: Status Quo - Today

The first COA of status quo does not implement any mitigations or resolutions to the non-compliant controls, attributes, or objectives that specifically map to the four primary concerns and issues. Therefore the 250 AFSPC mission systems supporting DOD warfighters from a space and cyberspace mission will continue to operate without any reduction to the cyber-attack surface as indicated in table 11. While this COA saves time, manpower, and financial resources in the short-run it does not minimize vulnerabilities to mission systems or minimize the impact to the operational mission provided by AFSPC to the warfighter and will be inherently lead to



LIKELIHOOD	Very High	🟩	🟩	🟨	🟧 I, P	🟥
	High	🟩	🟩	🟨	🟧 D	🟥 Rs,
	Mod	🟩	🟩	🟨	🟨	🟧 Rc
	Low	🟩	🟩	🟩	🟩	🟨
	Very Low	🟩	🟩	🟩	🟩	🟩
		Very Low	Low	Mod	High	Very High
	IMPACT					



LIKELIHOOD	Very High	🟩	🟩	🟨	🟧 I, P	🟥
	High	🟩	🟩	🟨	🟧 D	🟥 Rs,
	Mod	🟩	🟩	🟨	🟨	🟧 Rc
	Low	🟩	🟩	🟩	🟩	🟨
	Very Low	🟩	🟩	🟩	🟩	🟩
		Very Low	Low	Mod	High	Very High
	IMPACT					

Table 11. Risk Assessment Baseline (left) and COA 1 Impact (right)

mission failure across two of the three mission of the Air Force, that being to fly, fight, and win in air, space and cyberspace.

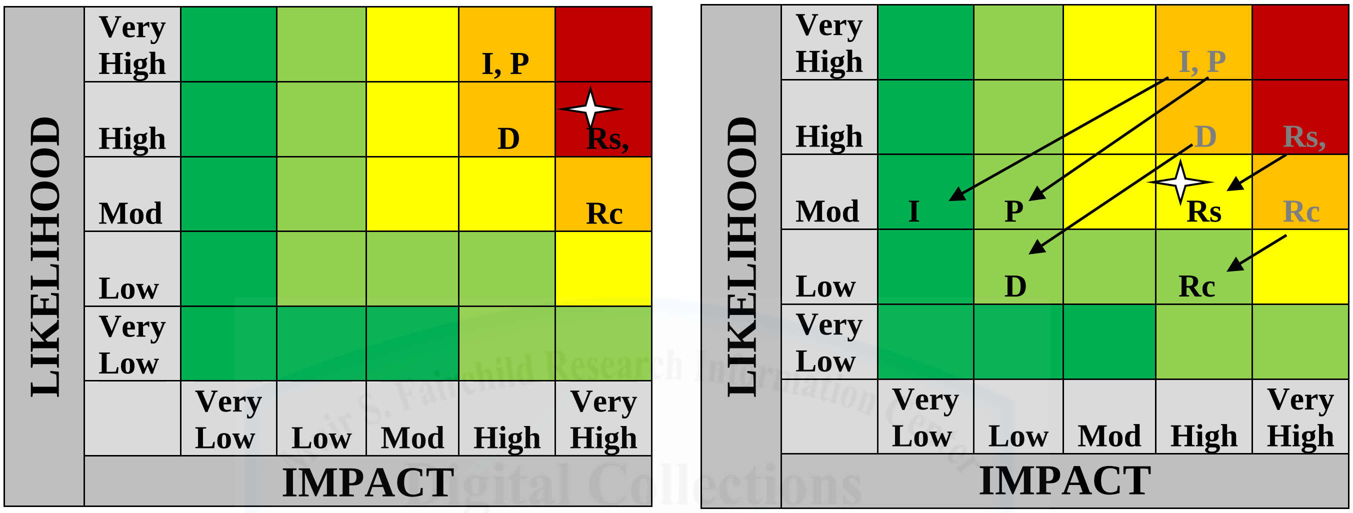
COA 2: AFSPC Solution – Short to Mid-Term

The second COA is short to mid-term and concentrates on AFSPC mitigations and/or solutions to the four primary concerns and issues. First, leadership must update AFSPC Instruction 33-202 policy to define continuous monitoring as a Tier III CSSP and mandate its communications squadrons shift from sustainers and maintainers of communication to defensive cyber operators who provide 24/7 monitoring and reporting. Under this construct, the 24/7 continuous monitoring provided by the defensive cyber operators will greatly improve the level of situational awareness through full network visibility which may potentially lead to a 90 percent improvement in its risk posture as identified by the USA Department of State.[30] Continuous monitoring directly effects both the Identify and Protect NIST functions to substantially draw down the overall risk and lower the cyber-attack surface. Second, AFSPC must address the lack of defense-in-depth in regards to the absence of a Tier II CSSP.

By financially resourcing and providing personnel to stand up a MAJCOM-wide Tier II CSSP for all mission systems, AFSPC will be able to positively impact both the Detect and Respond functions within NIST. According to the most recent DOD Cybersecurity Discipline Implementation Plan amended in February of 2016, one of the four primary lanes of effort to improve cybersecurity and reduce the cyber-attack surface is to implement Tier II CSSPs.[31] Furthermore, according to the Commander USCYBERCOM, “the department must move to a more agile and defendable posture that will enable the Department’s vision and strategy for US military forces as they execute their assigned missions in all operational environments” by aligning networks and information CSSPs as a “centrally controlled authority” to “thwart cybersecurity threats."[32] Third, AFSPC must address the inability for risk assessors to obtain specific threat intelligence due to security clearances.

AFSPC must standup a CYBERCON equivalent to FPCON to notify cybersecurity professionals when the threat changes. Upon notification, cybersecurity professionals will implement a playlist or checklist to further tighten down the system and reduce the attack-surface in response to the changing threat. For example, when the FPCON increases, security forces personnel increase their presence on gates, increase perimeter checks, and decrease the likelihood of drugs and bombs entering the base by using dogs. Similarly, when CYBERCON increases cybersecurity personnel will increase audit reviews on firewalls (i.e. gates), increase manual review of audit logs for anomalies (i.e., perimeter checks), and decrease the number of non-essential connections to mission systems, such as cleared defense contractor connections, to limit avenues of attacks (i.e., likelihood). By implementing CYBERCON, AFSPC will reduce the cyber-attack surface based on real-time threat data across the entire AFSPC portfolio and subsequently reduce the NIST function of Identify. Finally, AFSPC must prioritize all non-compliant controls for resolution and/or mitigate across the AFSPC enterprise.

AFSPC must develop a plan to rack-and-stack the number of moderate non-compliant risk controls, attributes, and objectives under the RMF construct which can easily number into the hundreds based on the granular nature of RMF. To do this, AFSPC should utilize the existing SANS critical security controls that pay the highest dividend to defending legacy and modern weapon and provide specific and actionable ways to reduce the cybersecurity attack surface from an enterprise perspective. To accomplish this, AFSPC must conduct a gap assessment to compare its current security stance to the recommendations of the SANS critical controls, implement the "first five and other quick win" critical controls, assign security personnel to analyze and understand quick wins to develop an enterprise-wide solution and finally plan for deployment of "advanced controls" throughout the AFSPC portfolio.[33] Once AFSPC institutes the above mitigations and resolutions for the four primary issues and concerns, the overall cybersecurity attack-surface will be significantly reduced from a high water mark of "Very High" to a high water mark of "Moderate" as indicated by the stars in table 12.



LIKELIHOOD					
Very High				I, P	
High				D	✦ Rs,
Mod					Rc
Low					
Very Low					
	Very Low	Low	Mod	High	Very High
	IMPACT				

LIKELIHOOD					
Very High				I, P	
High				D	Rs,
Mod	I	P		✦ Rs	Rc
Low		D		Rc	
Very Low					
	Very Low	Low	Mod	High	Very High
	IMPACT				

Table 12. Risk Assessment Baseline (left) and COA 2 Impact (right)

COA 3: DOD Enterprise-Wide Solution – Mid to Long-Term

The third and final COA is mid to long-term and concentrates on DOD mitigations and/or solutions to the four primary concerns and issues within AFSPC and across all services to stop the threat from traversing sister networks and missions systems to gain access to AFSPC mission systems as many of the DOD systems are connected for interoperability purposes. First, the DOD must consolidate and then realign the 150 plus cybersecurity regulations and polices identified in Figure 1 under the six steps of RMF shown in Figure 2 to allow cybersecurity professionals to easily follow and implement policy across the life cycle of mission systems. Additionally, the

DOD must define continuous monitoring to ensure all services are applying the necessary tool sets at the tactical and operational level to ensure Tier II CSSPs can communicate and share tool sets at the strategic level.

Furthermore, the DOD must standup Tier II CSSPs based on geographical location and functionality of the missions systems across all services where it makes sense. For instance, a Tier II CSSP should not exist MAJCOM by MAJCOM but by functionality such as the nuclear, command, control, and communications functionality that spans multiple Air Force MAJCOMS and multiple services within the DOD. Furthermore, once the Tier II CSSPs have been established, the DOD must consider bonuses to retain enlisted and officers from separating and obtaining contractor jobs based on their new skillsets.

When it comes to threat intelligence, the DOD must enlist the efforts of the National Security Agency and other intelligence organizations and develop a DOD-wide CYBERCON. This DOD-wide CYBERCON must include checklists or playbooks that are unique for varying mission system platforms such as aircraft, satellite, submarines and ships, and artillery for each service to initiate as the CYBERCON level increases. A DOD-wide CYBERCON will instantaneously reduce the cybersecurity attack-surface across the board and severely hinder US adversaries' ability to move laterally across DOD mission systems.

Finally, the DOD must identify the most critical controls to reduce the cybersecurity attack-surface and mandate all services procure the necessary funds and implement the processes, procedures, and architectural adjustments necessary to become compliant with these RMF controls and NIST 800-30 primary functions. These statuses of these most critical controls must be captured for each mission system and reported up through the individual service chief information officers and then to the DOD chief information officer with either a funded get well plan and associated timeline or a request for funding and assistance to close down the cybersecurity risk. By updating policy in regards to continuous monitoring, standing up functionally based CSSPs to address defense-in-depth, establishing a DOD-wide CYBERCON for various system platforms, and mandating compliance with the most critical controls, the DOD will drive down all five primary NIST functions in AFSPC and the DOD from a high water mark of “Very High” to a high water mark of “Low” as indicated by the stars in table 13.

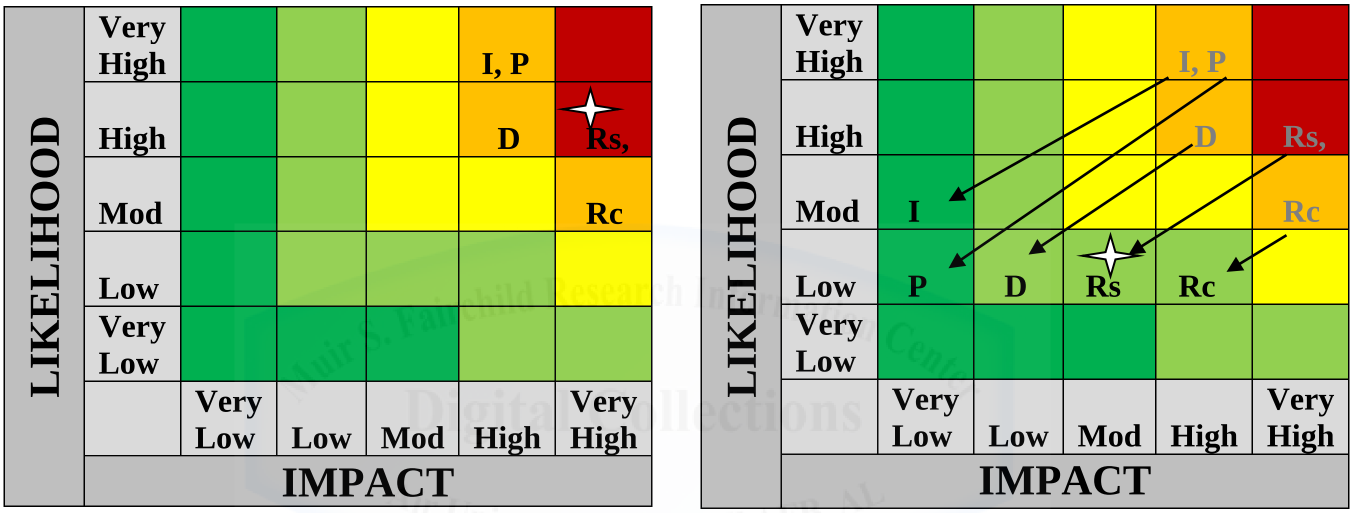


Table 13. Risk Assessment Baseline (left) and COA 3 Impact (right)

SECTION 6: RECOMMENDATION

An analysis of alternatives shows either no change in the cybersecurity attack-surface, to reducing the attack-surface from the high water mark of “Very High” risk to “Moderate” risk under the AFSPC solution, to reducing the attack-surface from the high water mark from “Very High” risk to “Low” risk under the DOD Enterprise-wide solution. While one may immediately point to the DoD Enterprise-wide solution as the recommendation based on the high-water mark of risk being “Low” vice “Moderate,” AFSPC cannot afford to wait on the mid to long-term solution and the DOD to possibly implement these changes across all services. The AFSPC Commander understands the current risk to US mission systems and knows the DOD has an overall cyber strategy to guide the development of its cyber forces to strengthen US cyber deterrence posture by establishing 130 National Mission Teams, Cyber Protection Teams and Support Teams by CY18. That is why General John E. Hyten, AFSPC/CC, has moved out and announced the command’s Space Enterprise Vision study in effort “to make the nation’s national security space enterprise more resilient” as “most US military space systems were not designed with threats in mind, and were built for long-term functionality and efficiency, with some systems operating for decades in some cases.”[34] The Space Enterprise Vision “accounts for the increasing threat to space systems, and provides a vision for how the Air Force should build a force responsive to that threat” and describes an “integrated approach across all space mission areas, coupling the delivery of space mission effects to the warfighter with the ability to protect and defend space capabilities against emerging threats.[35] COA 2 aligns with the AFSPC Commander’s Space Enterprise Vision and modifies policy to account for continuous monitoring by establishing defensive cyber operators in AFSPC communications squadrons to provide 24/7 monitoring and reporting of increased threats to space systems. COA 2 also establishes Tier II

CSSPs to address the Space Enterprise Vision of an integrated approach across all space mission areas and calls for the development of a MAJCOM wide CYBERCON to announce a change in threat and activate procedures for cybersecurity professionals to implement to protect and defend space capabilities against emerging threats. Finally, COA 2 addresses the most critical controls to ensure space mission effects to the warfighter are not interrupted or degraded. COA 2 is the short to mid-term solution to secure AFSPC mission systems for the warfighter now until the mid to long-term solution and the Space Enterprise Vision is developed and delivered to "maintain our nation's ability to deliver critical space efforts throughout all phases of conflict."[36]

SECTION 7: CONCLUSION

AFSPC must reduce the cybersecurity attack-surface for the nearly 250 space based systems by implementing cybersecurity to deter both adversarial nation-states and non-state actors from hindering the Air Force's ability to fly, fight, and win in air, space, and cyberspace. To deflect the thousands of cyber-attacks on AFSPC mission systems every day and to fulfill the AFSPC MISSION of "providing resilient and affordable space and cyberspace capabilities for the joint force and the Nation," AFSPC must utilize its communication's squadron Airmen to establish a 24/7 continuous monitoring capability to halt and report anomalies up the CYBER Command chain of command.[37] Additionally, these same Airmen will serve as cybersecurity professionals in Tier II CSSPs to provide defense-in-depth for space and cyberspace capabilities across the globe and team up with Airmen in the intelligence field who will deliver real-time threat data to influence the AFSPC CYBERCON decisions that will immediately reduce the cybersecurity attack-surface. Together, these Airman will fulfill the AFSPC VISION of "One team – innovative Airman fighting and delivering integrated multi-domain combat effects across the globe."[38] Finally, to meet AFSPC PRIORITIES of; "(1) Win today's fight, (2) Prepare for tomorrow's fight, and (3) Take care of US Airmen and Families," cybersecurity professionals must identify and implement the most critical RMF controls, objectives, and attributes.[39] By implementing the most critical controls, objectives and attributes to deter the very real cybersecurity threat effecting today's fight, and preparing for tomorrow's fight through the AFSPC Commanders Space Enterprise Vision, AFSPC will ensure the cybersecurity attack-surface is significantly reduced to ensure Airmen, their families, and the warfighter is taken care of and supported to the fullest extent possible.

NOTES

[1] Daniel Goure, Ph.D. "DoD's Cyber Perfect Storm: The Growing Threat Meets the Evolving Network," Lexington Institute, 29 July 2015, http://lexingtoninstitute.org/dods-cyber-perfect-storm-the-growing-threat-meets-the-evolving-network.

[2] *The National Strategy To Secure Cyberspace*, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, viii.

[3] The National Strategy, viii.

[4] The National Strategy, viii.

[5] U.S. Department of Defense, *Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[6] DOD *Cyber Strategy*.

[7] The DoD Cybersecurity Policy Chart, *Cyber Security & Information Systems Information Analysis Center*, 21 Aug 16, http://iac.dtic.mil/csiac/ia_policychart.html.

[8] Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2104, 2.

[9] DODI 8510.01, *Risk Management Framework (RMF).*

[10] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53Ar4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014, Appendix F, 96-98.

[11] Risk Management Framework, *Knowledge Service, Security Controls Explorer,* https://rmfks.osd.mil/rmf/General/SecurityControls/Pages/ControlsExplorer.aspx.

[12] Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Denfense (CND),* 9 February 2011, current as of 9 Jun 2015, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf, Enclosure B, 3-4.

[13] Shon Harris, "All In One Certified Information System Security Professional (CISSP)," Sixth Edition, McGraw Hill, 2013, 97.

[14] DODI 8510.01, Risk Management Framework (RMF), Enclosure 6, 34.

[15].DODI 8510.01, Risk Management Framework (RMF), Enclosure 6, 33.

[16] DODI 8510.01, Risk Management Framework (RMF), Enclosure 6, 46.

[17] DODI 8510.01, Risk Management Framework (RMF), Enclosure 6, 28.

[18] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, September 2012, Appendix G, Table G2.

[19] NIST 800-30, Table G3.

[20] NIST 800-30, Table G4.

[21] NIST 800-30, Table G5.

[22] NIST 800-30, Appendix H, Table H3.

[23] NIST 800-30, Appendix I, Table I2.

[24] NIST 900-30, Table I3.

[25] Executive Order, *Improving Critical Infrastructure Cybersecurity*, The White House Office of the Press Secretary, 12 February 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[26] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, 8-9.

[27]2015Annual Report on Security Clearance Determinations, National Counterintelligence and Security Center, *Advancing Counterintelligence and Security Excellence*, *http://www.fas.org/sgp/othergov/intel/clear-2015.pdf*, 4.

[28] System Administration, Networking, and Security (SANS) Institute, https://www.sans.org/.

[29] SANS.

[30] Enterprise Network Management iPost: *Implementing Continuous Monitoring at the Department of State*, v1.5, May 2010, http://www.state.gov/documents/organization/156865.pdf.

[31] DOD *Cybersecurity Discipline Implementation Plan*, October 2015, Amended February 2016, http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf.

[32] DOD *Cybersecurity Discipline Implementation Plan.*

[33] System Administration, Networking, and Security (SANS) Institute, *Center for Internet Security (CIS) Critical Security Controls: Guidelines Action Plan*, https://www.sans.org/critical-security-controls/guidelines.

[34] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*, 11 April 16, http://www.afspc.af.mil/News/Article-Display/Article/730817/afspc-commander-announces-space-enterprise-vision.

[35] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*.

[36] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*.

[37] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*.

[38] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*.

[39] AFSPC Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*.

BIBLIOGRAPHY

Air Force Space Command (AFSPC) Public Affairs, *AFSPC Commander Announces Space Enterprise Vision*, 11 April 16, http://www.afspc.af.mil/News/Article-Display/Article/730817/afspc-commander-announces-space-enterprise-vision.

Annual Report on Security Clearance Determinations, National Counterintelligence and Security Center, *Advancing Counterintelligence and Security Excellence*, 2015 http:www.fas.org/sgp/othergov/intel/clear-2015.pdf.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011, current as of 9 Jun 2015.

Department of Defense (DOD) *Cybersecurity Discipline Implementation Plan*, October 2015, Amended February 2016, http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf.

Department of Defense Instruction (DODI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2104.

Enterprise Network Management iPost: *Implementing Continuous Monitoring at the Department of State*, v1.5, May 2010, http://www.state.gov/documents/organization/156865.pdf.

Executive Order, *Improving Critical Infrastructure Cybersecurity*, The White House Office of the Press Secretary, 12 February 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Goure, Daniel, Ph.D. DoD's Cyber Perfect Storm: *The Growing Threat Meets the Evolving Network*, Lexington Institute, 29 July 2015, http://lexingtoninstitute.org/dods-cyber-perfect-storm-the-growing-threat-meets-the-evolving-network.

Harris, Shon, *All In One Certified Information System Security Professional (CISSP)*, 6th ed. Edition, McGraw Hill, 2013.

National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014, http://www.nist.gov/sites/default/files/Documents/cyberframework/cybersecurity-framework-021214.pdf.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, September 2012.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53Ar4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, December 2014.

Risk Management Framework, *Knowledge Service, Security Controls Explorer*, http://rmfks.osd.mil/rmf/General/SecurityControls/Pages/ControlsExplorer.aspx.

System Administration, Networking, and Security (SANS) Institute, *Center for Internet Security (CIS) Critical Security Controls: Guidelines Action Plan*, http://www.sans.org/critical-security-controls/guidelines.

The Department of Defense (DOD) Cybersecurity Policy Chart, *Cyber Security & Information Systems Information Analysis Center*, 21 Aug 16, http://iac.dtic.mil/Csiac/ia_policy chart.html.

The National Strategy to Secure Cyberspace, February 2003, http://www.us-cert.gov/sites/default/files//publications/cyberspace_strategy.pdf.

U.S. Department of Defense (DOD), *Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_For_web.pdf.